AO 91 (Rev. 11/11) Criminal Complaint

UNITED STATES DISTRICT COURT

for the

District of New Jersey

United States of America
v.
Zeeshan Khan

Case No. 20-mj-5659 (KMW)

Defendant(s)

CRIMINAL COMPLAINT

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of January 2020 to July 2020 in the county of Hudson in the _____ District of New Jersey, the defendant(s) violated:

Code Section	*Description of Offenses*
See Attachment A	

This criminal complaint is based on these facts:

See Attachment B.

☑ Continued on the attached sheet.

/s/ Emilio Gomez
Complainant's signature

Emilio Gomez, Task Force Officer
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 07/22/2020

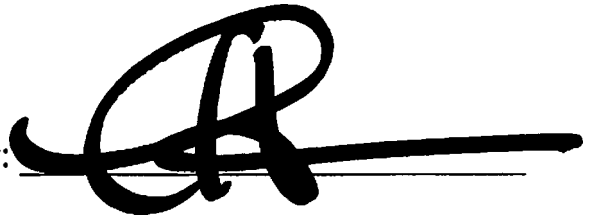
Judge's signature

City and state: District of New Jersey

Hon. Karen M. Williams, U.S. Magistrate Judge
Printed name and title

Print Save As... Attach Reset

CONTENTS APPROVED
UNITED STATES ATTORNEY

By: 

Meriah H. Russell
Special Assistant U.S. Attorney

Date: July 22, 2020

ATTACHMENT A

Count One – Wire Fraud Conspiracy

From in or about January 2020, through in or about July 2020, in the District of New Jersey and elsewhere, defendant ZEESHAN KHAN did knowingly and intentionally conspire and agree with Maaz Ahmed Shamsi and others to devise a scheme and artifice to defraud elderly victims, and to obtain money and property from the elderly victims thereof by means of materially false and fraudulent pretenses, representations, and promises, and, for the purpose of executing such scheme and artifice to defraud, did transmit and cause to be transmitted by means of wire communications in interstate and foreign commerce, certain writings, signs, signals, pictures, and sounds, contrary to Title 18, United States Code, Section 1343.

In violation of Title 18, United States Code, Section 1349.

ATTACHMENT B

I, Emilio Gomez, am a Detective with the New York City Police Department ("NYPD") and Task Force Officer ("TFO") with Homeland Security Investigation ("HSI"), New York, New York. I am familiar with the facts set forth herein based on my own investigation, my conversations with other law enforcement officers, and my review of reports, documents, and other evidence. Because this Complaint is being submitted for a limited purpose, I have not set forth each and every fact that I know concerning this investigation. Where statements of others are related herein, they are related in substance and in part unless otherwise indicated. Where I assert that an event took place on a particular date, I am asserting that it took place on or about the date alleged.

At all times relevant to this complaint:

BACKGROUND

1. The Department of Homeland Security ("DHS") / HSI, United States Postal Inspection Service ("USPIS"), Social Security Administration ("SSA"), Office of the Inspector General ("OIG"), and other agencies are investigating multiple criminal schemes perpetrated by individuals operating one or more call centers believed to be in India, who impersonate U.S. government officials, including SSA, and well-known businesses by "spoofing" legitimate phone numbers and sending recorded messages that are transmitted across the Internet to the phones of American consumers. These robocalls purport to be from federal government agencies, elements of foreign governments, and/or legitimate businesses, conveying alarming messages, such as: the consumer's Social Security number or other personal information has been compromised or otherwise connected to criminal activity; the consumer faces imminent arrest; their assets are being frozen; their bank and credit accounts have suspect activity; their benefits are being stopped; they face imminent deportation; or combinations of these things—all lies intended to induce consumers to speak to the fraudsters. When consumers answer the calls or return voicemail messages, the fraudsters offer to "resolve" these legal matters by immediate transfers of funds to settle the purported legal obligation, or to hold the consumer's assets only temporarily while the crisis resolves. In reality, the consumer is neither under investigation nor in legal jeopardy, and the same threatening robocall was made simultaneously to thousands of other U.S. consumers.

2. Investigation has revealed that from October 2018 to September 2019, the SSA alone received more than 465,000 complaints from U.S. consumers about callers impersonating SSA officials. Consumer losses associated with these complaints exceed $14 million. Similarly, the Federal Trade Commission ("FTC") estimates that more than 76,000 U.S. consumers filed complaints about fraudulent SSA impersonations, with estimated consumer losses reaching approximately $19 million between April 2018 and March 2019.

3. A second common technique used by the perpetrators involves refund fraud and remote computer access in which the unknown subject(s) gain remote access to the victims' computer. The scheme often consists of either a pop-up window on the victim's computer displaying a phone number to call for "Internet technical support services"; or the victim receives a telemarketing call informing the victim that their previously purchased anti-virus software is not up to date. The victim is then compelled to call the number displayed on the screen and/or follow the instructions of the tech support representative. Upon doing so, the victim is told that the anti-virus and/or protection he/she previously purchased was not sufficient for the victim's computer and, as a result, he/she is entitled to a refund. The unknown caller then states that the refund can be issued via wire into the victim's bank account. The victim is coerced into providing the unknown caller with remote access to his/her computer and the unknown perpetrators are able to move United States currency ("USC") from one of the victim's financial accounts to the victim's checking account, thus reflecting a significantly higher balance. As result of the transfer, the unknown caller advises the victim he/she was mistakenly overpaid and convinces the victim that he/she needs to send the money back via wire transfer and/or cash in the mail.

4. During March 2019, the Foundation for Worldwide International Student Exchange ("WISE") received information concerning participants in the Omni Orlando Championgate ("OMNI") Student and Exchange Visitor Program ("SEVIS") being involved in fraudulent activity. The students had obtained J-1 classification visas through the U.S. Department of State ("DSS") in coordination with US Citizenship and Immigration Services ("USCIS"). The purpose of the visas was to participate in programs for teaching, instructing or lecturing, studying, observing, conducting research, consulting, demonstrating special skills, receiving training, or to receive graduate medical education or training. OMNI served as a host organization / sponsor in the hospitality and tourism industry. According to the information provided to WISE, an exchange visitor involved in the program heard rumors that participating students were engaged in a bank fraud scheme. The exchange visitor explained that the fraud involved students being recruited by "dealers" to open multiple bank accounts with different financial institutions. The accounts

were then used to receive large wire transfers and the money was withdrawn by the students in the United States and provided to the "dealers" to be returned to India. Each participating student received a percentage of the money transfer. The exchange visitor further alleged that those participating in the fraud primarily originated from the Kolkata campus of the International Institute of Hotel Management ("IIHM") University in India.

5. This investigation has revealed that defendant ZEESHAN KHAN and Maaz Ahmed Shamsi were acting as money mules ("MM") for various fraud schemes whereby victims in the United States were defrauded out of their money and it was subsequently deposited via wire transfer into bank accounts operated by defendant ZEESHAN KHAN and Maaz Ahmed Shamsi. Defendant ZEESHAN KHAN was determined to be an Indian National born in August 1998. Defendant ZEESHAN KHAN arrived in the United States on November 2, 2019 via Philadelphia International Airport and was granted entrance into the U.S. with a J-1 non-immigration visa. Maaz Ahmed Shamsi, also an Indian National, was born in November 1996. Maaz Ahmed Shamsi arrived in the United States with defendant ZEESHAN KHAN on November 2, 2019 from DOHA International Airport in Qatar via Philadelphia International Airport, Philadelphia, Pennsylvania.

6. On November 18, 2019, defendants Maaz Ahmed Shamsi and ZEESHAN KHAN presented to the SSA Office in State College, Pennsylvania, to apply for their social security numbers. Defendant ZEESHAN KHAN and Maaz Ahmed Shamsi provided SSA with the same address[1] and telephone number. Defendant ZEESHAN KHAN and Maaz Ahmed Shamsi used their India Passports as proof of their identity and age, and their J-1 visas as proof of their legal alien status in the United States. Defendant ZEESHAN KHAN's passport ended in number 87096 and Maaz Ahmed Shamsi's passport ended in number 65686.

THE SCHEME TO DEFRAUD

7. On or about January 10, 2020, Maaz Ahmed Shamsi opened a checking account ending in 2565 with Truist Financial. Maaz Ahmed Shamsi provided an address in Boalsburg, Pennsylvania and presented his India passport ending in 65686 and his US Immigration Visa as identification. On January 22, 2020, Maaz Ahmed Shamsi received an $18,500 wire credit in his

[1] Both Maaz Ahmed Shamsi and defendant ZEESHAN KHAN indicated to SSA that they resided at 1 Country Club Lane, State College, Pennsylvania, 16803.

Truist Financial account from the US Bank account of VICTIM 1 of Maryville, TN. Similarly, on January 28, 2020, Maaz Ahmed Shamsi received a $19,500 wire credit into his Truist Financial account from the Bank of America account of VICTIM 2 of Annapolis, Maryland. US Bank and Bank of America attempted to recall the wire transfers from VICTIM 1 and VICTIM 2 because the wire transfers were fraud induced. However, prior to the wires being recalled, Maaz Ahmed Shamsi accessed approximately $37,975 of the stolen funds via international wire transfers to Hong Kong and South Korea and cash withdrawals conducted in and around State College, Pennsylvania.

8. On or about January 29, 2020, Citizens Bank was notified of a potential wire fraud involving the Citizens Bank account ending 7566[2] for Maaz Ahmed Shamsi. The account was opened by Maaz Ahmed Shamsi on January 10, 2020 in State College, Pennsylvania. On January 28, 2020, Maaz Ahmed Shamsi received a wire credit in the amount of $58,540 from the JPMorgan Chase Bank account of VICTIM 3 of Sterling Heights, Michigan. VICTIM 3 advised JPMorgan Chase Bank representative that the wire was sent as a result of a computer repair overpayment scam. The scam involved a suspect deceiving VICTIM 3 that VICTIM 3 was entitled to a refund for computer repairs; however, the suspect gained remote access to VICTIM 3's computer and coerced VICTIM 3 to send a wire with VICTIM 3's own funds. On January 29, 2020, Maaz Ahmed Shamsi withdrew the funds via in-branch cash withdrawal in State College, Pennsylvania in the amount of $5,600 and an outgoing international wire transfer in the amount of $52,465 to OCBC Wing Hang Bank in Hong Kong for the benefit of Wong How Kwun.

9. On or about February 3, 2020, a Manufacturers and Traders Trust (M&T) Bank investigator identified a $29,655 wire credit received by the M&T Bank account ending 85933 belonging to Maaz Ahmed Shamsi. The credit was received on January 30, 2020. The wire originated from the Bank of America account of VICTIM 4 of Apache Junction, Arizona. On January 31, 2020, Maaz Ahmed Shamsi visited the M&T Bank located in Bryant Park, New York and attempted to wire $26,000 to Hong Kong. Bank of America recalled Maaz Ahmed Shamsi's wire to Hong Kong and advised that it was the result of

---

[2] Maaz Ahmed Shamsi opened Citizens Bank account ending 7566 on January 10, 2020 in State College, Pennsylvania and provided an India address.

[3] Maaz Ahmed Shamsi opened M&T Bank account ending 8593 on January 10, 2020 and provided his India passport ending in 65686 as identification and an address of 134 E. Boal Avenue, Apt. 4, Boalsburg, Pennsylvania, 16827.

a fraudulent payment scam.

10. On or about March 20, 2020, law enforcement interviewed VICTIM 5 of Hartville, Ohio. VICTIM 5 was contacted by a tech company and spoke with an individual who identified himself as Maaz Ahmed Shamsi. VICTIM 5 was questioned about cancelling tech support services. VICTIM 5 was informed that the cancellation would result in a $400 refund. During the course of the conversation, VICTIM 5 provided the caller with remote access to VICTIM 5's computer and was made to believe that $40,000 was inadvertently transferred into VICTIM 5's account at Huntington National Bank. VICTIM 5 was instructed to return the funds less the $400 refund via a wire transfer. VICTIM 5 was provided with the name, address, and account number to send the overpaid funds. Law enforcement confirmed that VICTIM 5 entered the Huntington National Bank branch with hand written notes of where to wire the money. VICTIM 5 requested that Huntington National Bank send a wire in the amount of $39,000 to a TD Bank account ending in 45054 in the name of defendant ZEESHAN KHAN[5]. Huntington National Bank representatives confirmed that the $40,000 deposit into VICTIM 5's account was the result of an internal transfer from VICTIM 5's line of credit to VICTIM 5's checking account.

11. On or about March 30, 2020, VICTIM 6 of New York, New York, with the assistance of a friend, filed an online complaint with the NYPD. VICTIM 6 explained that on or before February 27, 2020, VICTIM 6 received a screen message on VICTIM 6's desktop computer about renewing a Mac support contract with a company named Tech Lite Connect. The screen message froze VICTIM 6's computer and provided a telephone number to call if VICTIM 6 did not wish to renew the contract. VICTIM 6 spoke with an individual who advised that VICTIM 6 was entitled to a $500 refund. VICTIM 6 was told the $500 refund would be transferred to VICTIM 6's bank account from JPMorgan Chase Bank. The caller requested remote access to VICTIM 6's computer in order to process the refund. VICTIM 6 was asked to enter VICTIM 6's name and the amount of the refund on a JPMorgan Chase online

---

[4] Defendant ZEESHAN KHAN opened TD Bank Account ending 4505 on February 11, 2020 and provided an address of 19 Wallis Avenue, Jersey City, New Jersey 07306. At some point in early February 2020, the defendants moved from State College, Pennsylvania to Jersey City, New Jersey.

[5] Of note, the caller identified himself as SHAMSI to Victim 5, but gave KHAN's name and bank information as the recipient of the overpayment refund.

transfer form. VICTIM 6 entered $500, but when VICTIM 6 submitted the form, the amount changed to $50,000. As such, VICTIM 6 believed that $50,000 was mistakenly deposited into VICTIM 6's Citibank account. The caller became verbally abusive and demanded the money be refunded. Law enforcement confirmed that the $50,000 was actually transferred from VICTIM 6's savings account into VICTIM 6's checking account. VICTIM 6 was provided with wire instructions to return $45,450 to Tech Lite Connect. The wire was initially to be sent to a Bank of China account in the name of H.Y. That initial wire was unsuccessful and VICTIM 6 was provided with alternate wire instructions. The alternate instructions called for a wire in the amount of $49,447.23 to a TD Bank account ending 4505[6] in the name of defendant ZEESHAN KHAN, 19 Wallis Avenue, Jersey City, New Jersey 07306.

12. On or about April 3, 2020, law enforcement conducted surveillance at 19 Wallis Avenue, Jersey City, New Jersey. The address was determined to be associated with multiple MMs identified as students of the IIHM in Kolkata, India. Law enforcement observed mail addressed to Maaz Ahmed Shamsi, 19 Wallis Avenue, PO Box 8366, Jersey City, New Jersey, from Citibank and Wells Fargo Bank. The address was also utilized by defendant ZEESHAN KHAN with respect to his account at TD Bank.

13. On or about April 4, 2020, law enforcement interviewed VICTIM 7 of Salisbury, Maryland. VICTIM 7 advised that during late February 2020, VICTIM 7 received a telephone call from a computer tech company located in New York that had previously provided VICTIM 7 with technical support service. VICTIM 7 was led to believe that the company had over refunded VICTIM 7 and the overpaid funds must be returned. The unknown caller instructed VICTIM 7 to wire $28,500 to a Citibank account number ending in 8766 and in the name of Maaz Ahmed Shamsi, PO Box 8366, Jersey City, New Jersey. Law enforcement determined that the overpaid funds were actually the result of an internal transfer between VICTIM 7's savings and checking account. Law enforcement reviewed records and photographs associated with a Citibank account number ending in 8766 and confirmed that the account was in the name of Maaz Ahmed Shamsi, 19 Wallis Avenue, Jersey City, New Jersey. Following the wire from VICTIM 7, funds were withdrawn in New York, New York; Jersey City, New Jersey; and Hoboken, New Jersey, respectfully.

14. On or about April 8, 2020, law enforcement interviewed VICTIM 8 of South Bend, Indiana. VICTIM 8 advised that during the week of February

---

[6] Defendant ZEESHAN KHAN opened the TD Bank Account ending in 4505 on February 11, 2020 and provided the address of 19 Wallis Avenue, Jersey City, New Jersey.

23, 2020, VICTIM 8 received telephone calls from a man who identified himself as "David Jove". "David Jove" represented that VICTIM 8 was entitled to a $500 refund and subsequently coerced VICTIM 8 to provide him with remote computer access. As a result of the remote access, VICTIM 8 believed that "David Jove" had inadvertently deposited a $50,000 refund into VICTIM 8's bank account. VICTIM 8 was instructed to return the overpaid funds via wire transfer. Victim 8 was provided information for a Capital One Bank account ending in 5807[7] and the name of Maaz Ahmed Shamsi in order to complete the wire transfer. "David Jove" claimed that the initial $49,500 wire transfer was held as a result of technical difficulties and coerced VICTIM 8 to send a second wire to Maaz Ahmed Shamsi in the amount of $49,500. Law enforcement reviewed Capital One records and confirmed the above described $49,500 wire transfers into Maaz Ahmed Shamsi's Capital One account ending 5807 on February 28, 2020 and March 3, 2020, respectfully. Following the wires from VICTIM 8, approximately $19,300 of the funds were withdrawn from various locations in New York, New York.

15. On April 14, 2020, Wells Fargo Bank identified an incoming $9,500 wire transfer from the JPMorgan Chase Bank account of VICTIM 9 of Racine, Wisconsin that was credited to the Wells Fargo Bank checking account ending in 2717 belonging to Maaz Ahmed Shamsi at 19 Wallis Avenue, Jersey City, New Jersey[8]. VICTIM 9 notified JPMorgan Chase Bank that he/she was the victim of a scam and account takeover. Following the receipt of the $9,500 wire into Maaz Ahmed Shamsi's Wells Fargo checking account ending in 2717, funds were withdrawn via several $700 ATM withdrawals on 4-14-2020, 4-15-2020, 4-20-2020, and 4-21-2020 in Jersey City, New Jersey. Purchases from the Wells Fargo checking account ending 2717 were also made to Lyft, 7-Eleven, and Remitly.

16. On or about April 25, 2020, law enforcement completed a review of call detail logs pertaining to Maaz Ahmed Shamsi and Verizon telephone number (646)988-6406. The call detail logs revealed communication between Maaz Ahmed Shamsi and other money mules identified during the course of this investigation, to include defendant ZEESHAN KHAN whose telephone

---

[7] Maaz Ahmed Shamsi opened Capital One bank account ending 5807 on February 8, 2020 and provided his India passport ending in 65686 as identification. Video surveillance from the opening of the account further confirmed that the account was opened by defendant MAAZ AHMED SHAMSI.

[8] Maaz Ahmed Shamsi opened Wells Fargo checking account ending 2717 on February 11, 2020 and provided his India passport ending in 65686 as identification.

number was determine to be (718)909-2474. Specifically, between on or about February 4, 2020 to on or about April 16, 2020, there were approximately 75 outbound calls from Maaz Ahmed Shamsi's cell phone to the cellular telephone number of defendant ZEESHAN KHAN. During the same period, there were approximately 126 incoming calls to Maaz Ahmed Shamsi's cellular telephone, which included voicemails, from defendant ZEESHAN KHAN's telephone number (718)909-2474. Additionally, between on or about February 11, 2020 and on or about March 8, 2020, Maaz Ahmed Shamsi sent approximately 25 outgoing text messages to defendant ZEESHAN KHAN's telephone number (718)909-2474. During the same period, Maaz Ahmed Shamsi received approximately 21 incoming text messages from defendant ZEESHAN KHAN's telephone number (718)909-2474. Although the nature of these text messages is not known to law enforcement, I know from my training and experience that money mules often use text messages as a means of identification and a way to provide information concerning bank accounts and incoming wire transfers. The call detail logs further revealed that Maaz Ahmed Shamsi used his cellular telephone to call numerous telephone numbers associated with financial institutions, to include, Northwest Savings Bank, M&T Bank, Capital One, Chase, First National Bank, Santander Bank, Citibank, Bank of America, Wells Fargo Bank, and TD Bank, respectfully.

17. On or about April 25, 2020, law enforcement reviewed Bank of America records that pertained to Maaz Ahmed Shamsi. The records revealed two outgoing wire transfers in the amount of $24,500 and $15,000 that totaled approximately $39,500. The outgoing wire transfers were sent on March 5, 2020 and March 10, 2020 to the account of Jed Silverman PC for "services." The wires were funded by cash deposits into Maaz Ahmed Shamsi's Bank of America account ending 7546[9]. Law enforcement determined that Jed Silverman PC was a law office located in Texas that represented MD Azad, a/k/a Azad Mohammad, who was arrested by the Federal Bureau of Investigation ("FBI"), Texas City Resident Agency on February 28, 2020. MD Azad was arrested with two other individuals for their involvement in an elder technical support fraud scheme that involved the mailing of cash to Federal Express ("FedEx") locations in the Southern District of Texas. MD Azad was linked to many other targets of this investigation and was identified as a student of the IIHM in Kolkata, India.

[9] Maaz Ahmed Shamsi opened Bank of America account ending 7546 on February 10, 2020 and provided his India passport ending in 65686 and US Visa as identification.

18. On or about April 30, 2020, law enforcement learned that VICTIM 10 of Marietta, Georgia was contacted on or before January 16, 2020 by an individual who claimed to be an employee of "My Tech Partners." The employee inquired if VICTIM 10 wanted to renew or cancel a tech support/security subscription. VICTIM 10 previously purchased security software from "My Tech Partners." VICTIM 10 opted to cancel the subscription. VICTIM 10 was transferred to another representative who requested remote access to VICTIM 10's computer to remove the software and to process a $1,200 refund. VICTIM 10 attempted to enter $1,200 on an online form for the refund, but the amount populated as $12,000. The representative demanded that VICTIM 10 return $10,500 due to the refund error. VICTIM 10 sent a $10,500 wire to an account in Bangkok, Thailand. Law Enforcement determined that the overpaid funds in VICTIM 10's account was the result of internal transfers between VICTIM 10's own accounts. The purported employee of "My Tech Partners" maintained remote control of VICTIM 10's computer and informed VICTIM 10 that there was an Internal Revenue Service ("IRS") investigation due to the size of the wire transfer. The representative convinced VICTIM 10 to become a partner in the company in order to avoid the IRS investigation. The representative made it appear as if a $1 million dollar deposit was made into VICTIM 10's savings account. The representative was allegedly entitled to a $30,000 commission for bringing VICTIM 10 into the company as a partner. The representative requested that VICTIM 10 send the commission payment to a BB&T account ending 159110 in the name of defendant ZEESHAN KHAN and VICTIM 10 complied.

19. On or about April 30, 2020, VICTIM 11 of Los Angeles, California. VICTIM 11 advised law enforcement agents that sometime during December 2019 he/she received a telephone call from a representative with Norton Security who advised that VICTIM 11 needed to update their subscription and that Victim 4 was entitled to a $400 refund. VICTIM 11 was coerced to provide remote computer access for the refund to be processed. A window displayed on VICTIM 11's computer and VICTIM 11 attempted to enter $400, but was made to believe that he/she inadvertently input $4,000. VICTIM 11 was instructed to return the overpaid funds by purchasing $4,000 worth of Google gift cards and providing the serial numbers on each card to the Norton Security representative. The scheme was repeated multiple times, each time VICTIM 11 was led to believe there was an overpayment of a refund and instructed to purchase and mail multiple gift cards. VICTIM 11 then received

---

[10] Defendant ZEESHAN KHAN opened BB&T Account ending 1591 on January 8, 2020 and provided his India passport ending in 87096 and a US Immigration Visa as identification.

a telephone call from another Norton Security representative who indicated that the prior representative was fired due to fraudulent activity. The new representative informed VICTIM 11 that he/she was entitled to a full refund for all of the gift cards. VICTIM 11 was again made to believe that overpayment of a refund occurred and was instructed to return the overpaid funds via wire transfers, as well as, via checks and cash sent via United Parcel Service ("UPS"). Included in the various payments sent by VICTIM 11 was a $14,100 wire transfer to the Capital One account of Defendant ZEESHAN KHAN ending 7194[11]. Following the incoming wire transfer, Defendant ZEESHAN KHAN was captured on video making multiple ATM withdrawals from the Capital One account in Jersey City, New Jersey on April 14, 2020 and April 15, 2020, respectfully.

20. On or about May 1, 2020, VICTIM 12 of Bozeman, Montana advised law enforcement that during late January 2020, VICTIM 12's computer froze and a message appeared on the screen with a telephone number to contact. VICTIM 12 called the number and was greeted by a tech support representative. The tech support representative indicated that he would repair VICTIM 12's computer and process a refund in the amount of $499.99. The tech support representative requested remote access to VICTIM 12's computer in order to process the refund. A payment window appeared on VICTIM 12's computer. VICTIM 12 attempted to manually enter $499.99, but the field populated as $49,499. VICTIM 12 believed that $49,499 was mistakenly refunded to his account and was instructed to return the funds. The tech support representative generated a word document on VICTIM 12's computer with the wire instructions to return the funds. The instructions included the routing number, bank account, and recipient's name. Law enforcement later determined that the overpaid funds was the result of internal transfers between VICTIM 12's own bank accounts. Law enforcement reviewed records that confirmed that on January 27, 2020, a PNC Bank account ending in 2252[12] in the name of defendant ZEESHAN KHAN, received a wire in the amount of $49,499 from the Manhattan Bank account of VICTIM 12. Following the wire transfer, on January 29, 2020, there were two separate cash withdrawals from defendant ZEESHAN KHAN's PNC Bank account ending in 2252 – one in the amount of $5,000 and the second in the amount of $2,700 at the PNC Branches in State College, Pennsylvania in the amount of $5,000. A second

---

[11] Defendant ZEESHAN KHAN opened Capital One account ending 7194 on February 11, 2020 and provided his India passport ending in 87096 as identification.

[12] Defendant ZEESHAN KHAN opened PNC account ending 2252 on December 24, 2019 and provided his India passport ending in 87096 as identification.

cash withdrawal the same day was completed in State College, Pennsylvania in the amount of $2,900. On February 17, 2020, defendant ZEESHAN KHAN attempted to send a $41,514 wire from his PNC account to an account with the Royal Bank of Canada belonging to Royal Textile Inc's. However, PNC Bank was alerted to the fraud and $41,626.45 was returned to Victim 12's bank before defendant ZEESHAN KHAN could complete this international wire transfer.

21. On or about May 1, 2020, law enforcement interviewed VICTIM 13 of Brooklyn, New York. VICTIM 13 stated that during the first week of April 2020, VICTIM 13 received a telephone call from representatives with Premium Tech Company, whose services VICTIM 13 had previously utilized. The caller advised that the software was out of date and VICTIM 13 was entitled to a $600 refund. In order to process the refund, the representative requested remote access to VICTIM 13's computer. A payment window appeared and VICTIM 13 was asked to input the refund amount. VICTIM 13's computer froze and zeros were added to the end of the refund amount. VICTIM 13 was made to believe that he/she was inadvertently overpaid and was instructed to return the overpaid funds. VICTIM 13 was instructed to wire the funds to the Capital One account ending in 7194 of defendant ZEESHAN KHAN, PO Box 16433, Jersey City, New Jersey. A review of Capital One account records confirmed the incoming wire transfer from VICTIM 13 on April 16, 2020, in the amount of $19,300. Following the incoming wire transfer, defendant ZEESHAN KHAN was captured on video making multiple withdrawals from the account in Jersey City, New Jersey, on April 16, 2020 and April 17, 2020, respectfully.

22. On or about May 13, 2020, law enforcement interviewed VICTIM 14 of Toledo, Ohio. VICTIM 14 advised that on January 21, 2020, an e-mail was received from noreply@microsoft-care.com, which indicated that the order for Windows Defender would appear on VICTIM 14's account / credit card as $299.99 from Microsoft Services LLC. VICTIM 14 did not recognize the charge and immediately contacted the telephone number displayed on the e-mail. VICTIM 14 spoke with an individual who identified himself as "Nick," and who coerced VICTIM 14 to provide remote computer access in an effort to process a $299.99 refund. VICTIM 14 followed "Nick's" instructions and a refund window appeared on VICTIM 14's computer. VICTIM 14 was made to believe $29,999 was inadvertently entered instead of $299.99. VICTIM 14 was instructed to return the overpaid funds totaling $29,459 via a wire transfer to the PNC Bank account of Maaz Ahmed Shamsi, ending in 5393[13]. Upon

[13] Maaz Ahmed Shamsi opened PNC bank account ending 5393 on December

further review, VICTIM 14 determined that the refund was actually funds that had been transferred between VICTIM 14's own accounts at Fifth Third Bank.

Following the wire transfer from VICTIM 14 on January 22, 2020, Maaz Ahmed Shamsi attempted to wire $25,600 to Wong How Kwun in Hong Kong from the PNC Branch in State College, Pennsylvania on January 23, 2020. Maaz Ahmed Shamsi initially described the beneficiary of the wire in Hong Kong as a "friend of his fathers". When a PNC bank representative questioned Maaz Ahmed Shamsi about the wire he received, he alleged it was from his aunt and was a loan for student expenses. PNC did not authorize the wire to Hong Kong and froze $25,702.80 in Maaz Ahmed Shamsi's bank account. However, prior to the account being frozen, Maaz Ahmed Shamsi made a $3,500 cash withdrawal and a $300 cash withdrawal in State College, Pennsylvania. PNC Bank contacted Maaz Ahmed Shamsi on January 28, 2020 and he then alleged that the wire transfer into his account on January 22, 2020 was the result of an online application he completed for a student loan that was subsequently wired into his account. PNC advised Maaz Ahmed Shamsi that Fifth Third Bank was seeking a recovery of the wire transfer and that he should return the cash he withdrew. Maaz Ahmed Shamsi did not comply with PNC's request to return the cash he had withdrawn.

23. On or about May 13, 2020, law enforcement interviewed the daughter of VICTIM 15 of Coronado, California. The daughter of VICTIM 15 stated that around February 20, 2020, VICTIM 15 received a telephone call from "Computer Support" regarding a refund for services rendered. The caller coerced VICTIM 15 to provide remote computer access in an effort to process the refund. A window refund window appeared and VICTIM 15 was made to believe that he/she inadvertently entered $30,000. VICTIM 15 was instructed to return the money via a wire transfer to defendant ZEESHAN KHAN's Wells Fargo bank account ending 5516[14]. Following the wire transfer, photographs of defendant ZEESSHAN KHAN showed him making multiple withdrawals from his Wells Fargo bank account ending 5516 in New York, New York on February

---

30, 2019 in State College, Pennsylvania, and provided his India passport ending in 65686 as identification.

[14] Defendant ZEESHAN KHAN opened Wells Fargo account ending 5516 on February 10, 2020 and provided his India passport ending in 87096 as identification and an address of 19 Wallis Ave, Floor 1, Jersey City, New Jersey 07306.

29, 2020 and March 2, 2020, respectfully.

24. On or about June 2, 2020, law enforcement interviewed VICTIM 16 of Gilroy, California. VICTIM 16 utilized the services of a tech support company named Premium Tech Support Incorporated to assist with computer issues. During April 2020, VICTIM 16 received an e-mail from techpremiusuprt9@gmail.com, which indicated that the yearly subscription was due in the amount of $499.99 and that the balance was going to be automatically deducted from VICTIM 16's account. VICTIM 16 contacted the telephone number for the Cancellation Department in an effort to cancel the subscription. VICTIM 16 was coerced to provide the Premium Tech Support representative with remote computer access. VICTIM 16 was made to believe that he/she received a $15,000 refund rather than the intended $499.99 refund. VICTIM 16 was instructed to return $5,000 via a wire to a Capital One bank account ending 7194, in the name of ZEESHAN KHAN at 19 Wallis Avenue, Jersey City, New Jersey 07306. VICTIM 16 was further instructed to return to the remaining funds via Zelle and Bitcoin to names and wallet numbers provided by the Premium Tech Support representative. It was determined that the $15,000 refund was actually an advance from VICTIM 16's Wells Fargo credit card.

25. On or about June 2, 2020, law enforcement reviewed documents provided by AirBnB pursuant to a grand jury subpoena. The documentation revealed that Maaz Ahmed Shamsi was registered under Guest ID Number ending 1945. The Guest ID was created on March 25, 2020 and was registered under a cellular telephone believed to be in the possession of Maaz Ahmed Shamsi. The documentation further revealed that Maaz Ahmed Shamsi had a reservation with two additional guests at 146 Manhattan Avenue, Apartment 25, Jersey City, New Jersey. The reservation began on May 5, 2020 and ended on June 4, 2020.

26. On or about June 3, 2020, law enforcement conducted surveillance outside of 146 Manhattan Avenue, Jersey City, New Jersey. The location was observed to be a large, multi-unit, apartment building. Law enforcement observed defendant ZEESHAN KHAN exit the building and walk to the Santander Bank located at 241 Central Avenue, Jersey City, New Jersey 07307. Defendant ZEESHAN KHAN attempted to conduct a transaction at the outdoor automated teller machine (ATM); however, defendant ZEESHAN KHAN appeared to experience difficulty and entered the branch to use the interior ATM. After completing the ATM transaction, defendant ZEESHAN KHAN was

observed taking a photograph of the transaction receipt. It is common practice for MMs, such as defendant ZEESHAN KHAN, to take photographs of receipts as proof that they made deposits into specific accounts in furtherance of the wire scheme.

27. On or about June 5, 2020, Maaz Ahmed Shamsi initiated another reservation through AirBnB and was determined to be staying at 157 Zabriskie Street, Jersey City, New Jersey. On June 16, 2020, law enforcement conducted surveillance outside of 157 Zabriske Street, Jersey City, New Jersey. Law enforcement observed defendant ZEESHAN KHAN exit the home with another MM known to this investigation. Defendant ZEESHAN KHAN and the other MM utilized the services of Lyft to travel to the Best Buy located at 125 18th Street, Jersey City, New Jersey, where both exited the vehicle and were observed picking up an unknown item.

28. On or about June 25, 2020, law enforcement conducted surveillance outside of 157 Zabriskie Street, Jersey City, New Jersey. Law enforcement observed Maaz Ahmed Shamsi exit the building and travel to the People's United Bank located at 250 Park Avenue, New York, New York. Law enforcement determined that Maaz Ahmed Shamsi attempted to open an account at People's United Bank by presenting his India passport, but Maaz Ahmed Shamsi's request was denied due to an expired Visa. After exiting the People's United Bank location, Maaz Ahmed Shamsi was observed entering the Valley Bank located at 350 Park Avenue, New York, New York, followed by the Bank of America located at 345 Park Avenue, New York, New York. While at the Bank of America, Maaz Ahmed Shamsi appeared to conduct an ATM transaction.

29. On or about June 29, 2020, law enforcement interviewed VICTIM 17 of Stony Point, New York. During late May 2020, VICTIM 17 was contacted by a computer company regarding the purchase of a software plan for $449.98. On or about June 9, 2020, VICTIM 17 received a telephone call from a male who identified himself as "Steve," an employee of "Business Info Solutions." "Steve" represented that VICTIM 17 was entitled to a refund for the software purchase. VICTIM 17 provided "Steve" with remote computer access in order to complete the refund. VICTIM 17 was told to enter $450, but "Steve" claimed that VICTIM 17 had entered $45,000. "Steve" opened VICTIM 17's Citibank account on the computer so that VICTIM 17 could see the $45,000 deposit. "Steve" claimed that he would lose his job if VICTIM 17 did not return the funds. VICTIM 17 wanted to return the entire deposit, but "Steve" indicated that the bank would not allow it and instructed VICTIM 17 to wire $10,000 to the JPMorgan Chase Bank account of defendant ZEESHAN KHAN. "Steve" subsequently changed his mind and provided VICTIM 17 with alternate

instructions to send the $10,000 wire transfer to the Santander Bank account ending 5185 for defendant ZEESHAN KHAN, 19 Wallis Avenue, Jersey City, New Jersey15. After completing the wire transfer as instructed, VICTIM 17 learned that the refund came from another one of VICTIM 17's accounts with Citibank. Law enforcement reviewed Santander Bank records and confirmed that defendant ZEESHAN KHAN's account ending 5185 received the incoming wire transfer on June 11, 2020 in the amount of $10,000.

30. On or about June 29, 2020, law enforcement interviewed VICTIM 18 of Massapequa Park, New York. VICTIM 18 was a customer of Trend Microsystems, a computer support company based in the Philippines. On June 5, 2020, VICTIM 18 received an e-mail from AV Trend Micro Solutions LLC, info@trndmicrosolutions.xyz, and believed the e-mail to have originated from Trend Microsystems. The e-mail purported to be a Security Activation Invoice for Prime Titanium Maximum Security for a term of five years for three devices. The cost for the service was $392.95. The e-mail further indicated that VICTIM 18's credit card would be charged unless VICTIM 18 contacted the cancelation department. VICTIM 18 called the provided telephone number and requested cancelation of the service and a refund. VICTIM 18 was transferred to another department and told that a full refund would be provided and malware would be removed from VICTIM 18's computer. A Chase Deposit form appeared on VICTIM 18's computer and VICTIM 18 was instructed to enter $500 for the refund. After entering $500 the representative claimed that VICTIM 18 had entered $50,000 and the money was refunded to VICTIM 18's account at Capital One Bank. The representative alleged that he was going to lose his job and requested that VICTIM 18 return the overpaid funds via a wire transfer. VICTIM 18 was provided with wire instructions that the representative printed out on VICTIM 18's computer. Law enforcement obtained copies of the wire instructions from the Nassau County Police Department and confirmed that VICTIM 18 was instructed to send a wire transfer in the amount of $49,400 to the Santander Bank account ending 5185, for defendant ZEESHAN KHAN, 19 Wallis Avenue, 07306. After sending the wire transfer, VICTIM 18 realized that the refund was actually an internal transfer from VICTIM 18's money market account. Law enforcement reviewed Santander Bank records and confirmed that defendant ZEESHAN KHAN's account ending 5185 and received the incoming wire transfer on June 8, 2020 in the amount of $49,400.

31. On or about June 30, 2020, law enforcement interviewed VICTIM

---

15 Defendant ZEESHAN KHAN opened Santander Bank account ending 5185 on May 20, 2020 and provided his India passport ending in 87096 and US Visa as identification.

19 of Palmerton, Pennsylvania. VICTIM 19 ordered a new computer via cellular telephone during April 2020. A few weeks after placing the order, VICTIM 19 was contacted and notified that the company was going out of business and VICTIM 19 was entitled to a $300 refund for his computer purchase. The caller gained remote access to VICTIM 19's computer and instructed VICTIM 19 to enter the $300 refund amount. The amount changed to $30,000 and VICTIM 19 overheard the caller speaking with his supervisor stating that he was going to be fired. The caller directed VICTIM 19 to wire transfer $29,600 to the Santander Bank account of Maaz Ahmed Shamsi. VICTIM 19 traveled to the local First Northern Bank branch and called the bank from the parking lot to initiate the wire transfer. VICTIM 19 had never before sent a wire transfer and due to the COVID-19 Quarantine, VICTIM 19 was unable to enter the bank. A bank representative met with VICTIM 19 in the parking lot and completed the necessary paperwork to initiate the wire transfer. Law enforcement obtained copies of the wire instructions from the Palmerton Police Department and confirmed that VICTIM 19 was instructed to send a wire transfer in the amount of $29,600 to the Santander Bank account ending 0321[16] for Maaz Ahmed Shamsi, 44 Logan Avenue, Jersey City, New Jersey 07306. After the wire transfer was completed, it was determined that the refund was an internal transfer between VICTIM 19's own accounts with First Northern Bank. Law enforcement reviewed Santander Bank records and confirmed Maaz Ahmed Shamsi's account ending 0321 received the incoming wire transfer on May 1, 2020 in the amount of $29,600. Following the incoming wire on May 1, 2020, Maaz Ahmed Shamsi made approximately eleven cash withdrawals at various locations in Jersey City, New Jersey on May 1, 2020 and May 4, 2020.

32. As detailed above, between on or about January 22, 2020 to in or about June 11, 2020, defendant ZEESHAN KHAN and Maaz Ahmed Shamsi received or attempted to receive more than $618,000 in furtherance of the wire fraud conspiracy. The transactions detailed above are more generally summarized as follows:

VICTIM	**DATE**	**WIRE AMT**	**MONEY MULE**	**RECEIVING BANK**
VICTIM 1	01-22-2020	$18,500	Maaz Ahmed Shamsi	TRUIST FINANCIAL
VICTIM 2	01-28-2020	$19,500	Maaz Ahmed	TRUIST

[16] Maaz Ahmed Shamsi opened Santander Bank account ending 0321 on February 11, 2020 and provided his India passport ending in 65686 and his US Visa as identification.

			Shamsi	FINANCIAL
VICTIM 3	01-28-2020	$58,540	Maaz Ahmed Shamsi	CITIZENS BANK
VICTIM 4	01-30-2020	$29,655	Maaz Ahmed Shamsi	M&T BANK
VICTIM 5	02-28-2020	$39,000	ZEESHAN KHAN	TD BANK
VICTIM 6	03-02-2020	$49,447.23	ZEESHAN KHAN	TD BANK
VICTIM 7	03-06-2020	$28,500	Maaz Ahmed Shamsi	CITIBANK
VICTIM 8	02-28-2020	$49,500	Maaz Ahmed Shamsi	CAPITAL ONE BANK
VICTIM 8	03-03-2020	$49,500	Maaz Ahmed Shamsi	CAPITAL ONE BANK
VICTIM 9	04-14-2020	$9,500	Maaz Ahmed Shamsi	WELLS FARGO BANK
VICTIM 10	01-23-2020	$30,000	ZEESHAN KHAN	BB&T BANK
VICTIM 11	04-14-2020	$14,100	ZEESHAN KHAN	CAPITAL ONE BANK
VICTIM 12	01-27-2020	$49,499	ZEESHAN KHAN	PNC BANK
VICTIM 13	04-16-2020	$19,300	ZEESHAN KHAN	CAPITAL ONE BANK
VICTIM 14	01-22-2020	$29,459	Maaz Ahmed Shamsi	PNC BANK
VICTIM 15	2-28-2020	$30,000	ZEESHAN KHAN	WELLS FARGO BANK
VICTIM 16	4-21-2020	$5,000	ZEESHAN KHAN	CAPITAL ONE BANK
VICTIM 17	06-11-2020	$10,000	ZEESHAN KHAN	SANTANDER BANK
VICTIM 18	06-08-2020	$49,400	ZEESHAN KHAN	SANTANDER BANK
VICTIM 19	05-01-2020	$29,600	Maaz Ahmed Shamsi	SANTANDER BANK
	TOTAL	$618,000.23		